ACUITY SOLUTIONS

ACUITY
Your Vision | Our Focus

ZERO TRUST

Preemptive, proactive cyber security

The Administration's Cyber Executive Order dramatically shifts security focus from infrastructure to what really matters: data and operations.

How Does the Zero Trust Framework Tighten Security?

Traditional, perimeter-based IT security is no longer a viable option for federal agencies. As cloud and mobility have taken hold, problems with the scalability and sustainability of the outdated security model have grown exponentially. Zero Trust builds on a basic premise: trust nothing and no one. Always assume your network is compromised, and focus on protecting your data at the level it needs protecting. Zero Trust is not a specific technology – it's a complex framework.

Identity management and knowing your data are central. The network is segmented at a granular level (micro-segmentation), based on workflow. Users are no longer authorized at the network level: they are authenticated based on their role, the state of the device they use, and the functions they are allowed to perform.

> *No matter where you are in your journey, Acuity experts can help you meet the requirements of the White House Executive Order and dramatically mature your security posture.*

Data is categorized or tagged, and its movement is controlled. Data is encrypted when stored and while in transit to further protect it. These Zero Trust protections allow an organization to control who accesses data, when, from where, and under what conditions.

THREAT VECTOR CHANGES ARE CONSTANT. DEFEND YOUR AGENCY TODAY.

BASELINE

Assess network activity traffic and behaviors and identify sensitive/mission-critical data

GAP ANALYSIS

Identify high value systems and map Zero Trust capabilities to technical controls

ROADMAP

Prioritize key activities, actions, dependencies, outcomes and offer a communications plan for stakeholder reporting

Stakeholder inclusion

Tools

- DoD reference architecture
- CISA Zero Trust Maturity Model (ZTMM) v2.0
- NIST 800-53 controls
- Mitre ATT&CK Framework

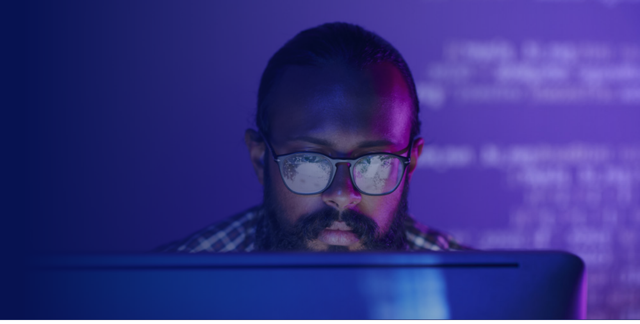
Common Recommendations

- Use AI/ML to predict threats
- Manage and secure APIs
- Apply phishing-resistant multifactor authentication at the application level
- Apply security capabilities closer to the data/application

LEARN MORE | www.myacuity.com

ACUITY SOLUTIONS

ZERO TRUST



Zero Trust optimizes security resources. With Zero Trust, security capabilities are moved closer to data rather than individuals. This means organizations can focus security resources where they are most needed and allow users who work with less sensitive data to have fewer security "hoops" to jump through.

Acuity has helped the Government define Zero Trust core principles and put them into practice. We are ready to help your organization:

Take a strategic approach to achieving a Zero Trust architecture

Base your Zero Trust journey on agency mission needs

Understand how to develop a phased path, with impactful early wins

Devise targeted plans and achieve longer-term Zero Trust goals

Acuity participates in government-wide activities working towards Zero Trust.

Acuity is actively working across the U.S. Government to assist agencies in their journey to Zero Trust. We worked with **CISA and NIST** in the creation of an initial Zero Trust overlay mapping to the SP 800-53 control. Additionally, Acuity is supporting the government and **ATARC** as they work directly with industry, reviewing their Zero Trust capabilities relative to the government's defined and documented requirements.

Acuity brings best practices and applies them to your specific agency needs.

CASE 1

Acuity helped an Agency department increase efficiencies and improve security by moving to the AWS cloud. However, their API structure – which relied on personally identifiable information (PII) – required tightened security protocols to limit accessibility. Acuity built custom API integrations that no longer relied on PII and expanded the use of the client's multifactor authentication platform.

CASE 2

Acuity uses FedRAMP documentation and assessment of inherited controls, along with our proprietary cyber hygiene process to build enterprise-wide comprehensive security strategy and policies. This process helped our customer transform its networks and automate the secure deployment of cloud infrastructure. Our teams designed and provided a robust governance framework to ensure app development teams meet security requirements. We developed mechanisms for continuous evaluation of new capabilities, incorporating security throughout the process without slowing development.

CASE 3

Acuity developed System Security Plans to meet FISMA compliance objectives and used our NIST SP 800-37-based Security Assessment and Authorization (SA&A) procedures to close material weaknesses related to agency processes. We integrated disaster recovery and contingency planning activities and leveraged standardized security templates and Continuous Diagnostics and Mitigation (CDM) procedures to support each Assessment and Authorization (A&A) process, to ensure systems meet security configuration standards throughout the lifecycle.

Acuity, Inc. is a leading federal technology consulting firm headquartered in Reston, VA. Acuity provides deep domain and technical expertise to help clients optimize mission effectiveness.

LEARN MORE | www.myacuity.com

Kristin Cooke, *VP, Business Development* | bd@myacuity.com | (703) 766-0977

ACUITY
Your Vision | Our Focus